Advisory Alert

Alert Number: AAA20210901 **Date:** September 1, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Multiple Vulnerabilities
Node.js	**High**	Multiple Vulnerabilities

Description

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22555, CVE-2021-32399, CVE-2021-3609, CVE-2021-22543, CVE-2020-27777, CVE-2021-29154, CVE-2021-29650, CVE-2021-3621, CVE-2020-8648)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exist with Redhat products. kpatch-patch security update, kernel security bug fix update,sssd shell command injection. **CVE-2021-3621** - The System Security Services Daemon (SSSD) service provides a daemon for managing access to remote directories and authentication mechanisms. It also provides system name transfer and Pluggable Authentication verification module interfaces, and a pluggable back-end system to connect to multiple other account sources.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux for Power,endian Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Virtualization Host 4 for RHEL 7 x86_64 Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.2 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:3381 https://access.redhat.com/errata/RHSA-2021:3375 https://access.redhat.com/errata/RHSA-2021:3327 https://access.redhat.com/errata/RHSA-2021:3328 https://access.redhat.com/errata/RHSA-2021:3365 https://access.redhat.com/errata/RHSA-2021:3365 https://access.redhat.com/errata/RHSA-2021:3365

Affected Product	**Node.js**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-37701, CVE-2021-37712, CVE-2021-37713, CVE-2021-39134, CVE-2021-39135)
Description	Node.js has released Security Updates addressing multiple vulnerabilities that exist with Arbitrary File Creation, Arbitrary File Overwrite, and Arbitrary Code Execution via insufficient symlink protection due to directory cache poisoning using symbolic links. This logic was insufficient when extracting tar files that contained both a directory and a symlink with the same name as the directory. This order of operations resulted in the directory being created and added to the node-tar directory cache. When a directory is present in the directory cache, subsequent calls to mkdir for that directory are skipped.
Affected Products	All versions of the 14.x, and 12.x releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/aug-2021-security-releases2/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.